

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF A BLACK
APPLE iPhone IN A BLACK OTTERBOX CASE
THAT IS CURRENTLY LOCATED AT THE USPIS
EVIDENCE LOCKER, 850 TWIN RIVERS DRIVE,
ROOM 307, COLUMBUS, OH 43216

Case No. 2:24-mj-194

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Tyler Fink, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a United States Postal Inspector, having been so employed since April of 2022. I am presently assigned to the Columbus, Ohio Field Office, Pittsburgh Division of the United States Postal Inspection Service (“USPIS”).

3. I have gained experience through completion of the Basic Inspector Training (“BIT”) in August of 2022. During BIT, I was instructed in all phases of criminal investigation, such as criminal law, search and seizure, field enforcement techniques, firearms proficiency, drug and narcotics identification, drug, and narcotics field testing, and interviewing and evidence collection. Since August 2022, I have worked with various federal, state, and local law enforcement agencies in the investigation of crimes involving the U.S. Mail and the U.S. Postal Service (“USPS”), including but not limited to mail fraud, bank fraud, mail theft, burglaries, robberies, dangerous mail investigations, and mailed narcotics.

4. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

5. The facts contained in this affidavit are based on my personal knowledge as well as that of the other agents involved in this investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is a black Apple iPhone in a black Otterbox case that was taken from the center console of a vehicle during a traffic stop of Antonio Peake conducted on January 12, 2024, hereinafter, the “Device.” The Device is currently located at the USPIS Evidence Locker, 850 Twin Rivers Drive, Room 307, Columbus, Ohio 43216.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

The Check-Stealing Scheme

8. Law enforcement has been investigating a network of individuals involved in robbing or stealing USPS-issued Arrow Keys from USPS employees in Central Ohio. The criminal actor(s) focus on stealing these Arrow Keys, which open USPS collection boxes, for the purpose of stealing the mail located within.

9. The criminal actor(s) typically visit USPS collection boxes during the night/early morning. The criminal actor(s) use the stolen Arrow Keys and other methods to gain access to the USPS collection boxes, remove the mail, and then leave the area.

10. The criminal actor(s) generally take checks from the stolen mail, then alter those checks and deposit, or attempt to deposit, the counterfeit checks into various bank accounts. The criminal actor(s) often conceal the source of the money by transferring the fraudulently obtained money to other bank accounts. The criminal actor(s) then attempt to deplete the fraudulently obtained money via ATM withdrawals, peer-to-peer transactions, and/or the purchase of cryptocurrency. Generally, the initial actor who steals the Arrow Key works with other individuals to accomplish the objectives outlined above.

Robbery Details

11. On or about June 21, 2023, at approximately 2:14PM, a USPS Letter Carrier was delivering mail near 86 Linda Court, Westerville, Ohio, when an unknown male black suspect approached the carrier and initially said something the carrier was unable to understand. The suspect then said, "you know what this is," and demanded the carrier's keys and wallet. The suspect lifted the front of his shirt revealing what the carrier believed to be the hand grip of a firearm wrapped in a black plastic bag. The carrier initially tried to give the suspect his vehicle key but the suspect responded, "no, the other key," referring to the USPS Arrow Key. The suspect then took the carrier's USPS Arrow Key and wallet and fled in a grey sedan.

Use of a Westerville Postal Key

12. On November 1, 2023, Inspectors observed via photo surveillance multiple suspects accessing the blue collection box located at the Westerville Main Post Office, 617 McCorkle Boulevard, Westerville, Ohio. A key matching the series from the Westerville Main Post Office would be needed to access these collection boxes. A still-frame photo of that activity is depicted below:



Through electronic surveillance, Inspectors determined the box was targeted at approximately 12:12AM, 34 minutes after the timestamp indicated on the recovered photo.

13. On November 6, 2023, Inspectors observed via photo surveillance multiple suspects accessing the same blue collection box located at the Westerville Main Post Office. A key matching the series from the Westerville Main Post Office would be needed to access these collection boxes. A still-frame photo of that activity is depicted below:



Through electronic surveillance, Inspectors determined the box was targeted at approximately 12:13AM, 26 minutes before the timestamp indicated on the recovered photo.

14. On November 13, 2023, Inspectors observed via photo surveillance multiple suspects accessing the same blue collection box located at the Westerville Main Post Office. A key matching the series from the Westerville Main Post Office would be needed to access these collection boxes. A still frame photo of that activity is depicted below:



Through electronic surveillance, Inspectors determined the box was targeted at approximately 1:24AM, 28 minutes before the timestamp indicated on the recovered photo.

15. On November 28, 2023, Inspectors observed via photo surveillance multiple suspects accessing the same blue collection box located at the Westerville Main Post Office. A key matching the series from the Westerville Main Post Office would be needed to access these collection boxes. A still frame photo of that activity is depicted below:



Through electronic surveillance, Inspectors determined the box was targeted at approximately 3:18AM, 28 minutes before the timestamp indicated on the recovered photo.

Interview of Antonio Peake

16. On July 11, 2023, Inspector Fink was contacted by Westerville Police Department regarding Antonio Peake, who was found to be in possession of fraudulent checks. Inspectors Fink and Massaro read Peake his *Miranda* Rights, which he waived prior to being interviewed. Peake stated that he bought the checks for his own use via Telegram and received them through the mail. I know that stolen checks and instruments used to carry out fraudulent activities can be purchased on social media sites such as Telegram and Instagram, both being accessible via the web or phone applications. Peake stated that he paid for the checks using CashApp in which he sent bitcoin to a wallet/address. During the interview, Peake was asked about the blank checks he had and stated he knows how to make checks from practicing.

Arrest of Antonio Peake

17. On January 12, 2024, Antonio Peake was arrested following a traffic stop by the Dayton Police Department because he had an active warrant for his arrest for receiving stolen property out of Franklin County. This warrant related to the incident with Peake on July 11, 2023, when he was found in possession of fraudulent checks as he attempted to pay for a hotel with cards not in his name. At the time of Peake's traffic stop and arrest, he was accompanied by two other individuals – Jaylen L. Murphy and Kevon E. Mayers. Murphy was in the front passenger seat and Mayers was seated in the rear driver's side seat. During the traffic stop, officers ran a K9 unit on the vehicle, and that K9 alerted to the presence of illegal narcotics. As a result, officers conducted a search of the vehicle.

18. During that search, officers seized the following items: (1) an Apple Laptop Computer (S/N: A2159 – FVFZMESPL40Y) from the rear seat; (2) a silver/gray Apple iPhone with a cracked back from the rear seat; (3) a black Apple iPhone in a gold-colored case from the rear seat; (4) a black Apple iPhone in a black Otterbox case from the front center console; (5) approximately 1,700 checks from various locations such as Columbus and Westerville, including fraudulently produced checks and altered checks; and (6) various banking documents, social security cards, and other personal identification using multiple names, addresses, and photos of individuals. Some of these documents appear to have corresponding names to those on what appear to be stolen checks, and the same photo was used to create different identities. Many of the recovered checks were dated with days that align with known dates the McCorkle Post Office collection boxes were targeted, as outlined above. Additionally, victims have been able to provide mailing information to help verify when they deposited the checks in the mail system and where.

Use of Cell Phones and Computers

19. In my training and experience, I know that criminals who commit robberies and mail theft often carry cellular devices and will use them to communicate with other criminal participants to coordinate plans and logistics with each other and/or to navigate to and away from certain locations, including the site(s) of the robberies or the mail theft. I also know from my training and experience that “cell phones and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society.”

Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quotation omitted). It is therefore likely that the suspects in the postal robbery and mail theft described above were carrying cellular devices and communicated with each other or other unknown participants via those devices prior to or after the robbery and mail theft took place and/or used those devices for navigation purposes.

20. In my training and experience, I also know that criminals who participate in the check-cashing scheme described above commonly use computers to generate fake IDs, checks, and other articles to carry out the scheme. Furthermore, the fake Ohio Bureau of Motor Vehicles interim documentation articles found within the vehicle that Peake was driving could be used as means to present during bank transactions. These documents appear to be created using theft victims' information, presumably from their checks, to make what appear to be legitimate documents, such as the BMV paperwork and receipts from various businesses. Additionally, at the time of this writing, two victims have stated their checks have been counterfeited. Both the IDs and checks are documents that can be generated using various platforms that can be found on computers, such as Microsoft Office products and Adobe products, where files can be altered. Computers can also be used to access sites such as Instagram or Telegram, which I know to be sites where fraudulent activities are coordinated among suspects. These activities can include buying and selling checks and IDs, and more generally selling/purchasing stolen mail.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and

presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that cellular devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and personal digital assistant, which stores names, addresses, appointments, and notes, among other information. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the device. I also know that GPS navigation devices that determine location and assist in navigating to specific locations can uncover, among other things, evidence that reveals or suggests who possessed or used the device and information about specific locations that may be relevant in a criminal investigation.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

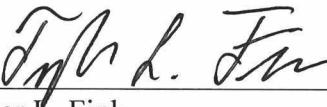
25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

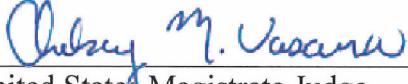
CONCLUSION

27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B as those items constitute evidence of violations of 18 U.S.C. § 2114 (robbery of mail, money, or other property of the United States); 18 U.S.C. § 1704 (possession of stolen postal keys); and 18 U.S.C. § 1708 (mail theft).

Respectfully submitted,



Tyler L. Fink
Postal Inspector
United States Postal Inspection Service



United States Magistrate Judge
Columbus, Ohio